La decisione della Corte Costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione – un rapporto sul caso BVerfGE, NJW 2008, 822

La decisione della Corte Costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione – un rapporto sul caso BVerfGE, NJW 2008, 822

14 Novembre 2009 | Abel Wiebke |

di **Wiebke Abel** – Ricercatore associato, SCRIPT; dottorando in Giurisprudenza presso l'Università di Edimburgo; LLM, Università di Edimburgo (2006) e **Burkhard Schafer** – Professore presso l'Università di Edimburgo, Dipartimento di Giurisprudenza.

Traduzione di **Antonella Piccinin** – Università LUISS Guido Carli, Roma.

Abstract.

Il 27 febbraio 2008, la Corte Costituzionale Federale tedesca (Bundesverfassungsgericht), per la prima volta, ha riconosciuto in una decisione storica un nuovo diritto costituzionale alla riservatezza ed integrità dei sistemi tecnologici d'informazione. In questo commento al caso mostreremo perché la Corte ha considerato necessario introdurre una nuova normativa e verrà fornita una visione d'insieme del nuovo diritto costituzionale così stabilito.

1. *Introduzione*

Il 27 febbraio 2008, la Corte Costituzionale Federale tedesca (Bundesverfassungsgericht)[1] per la prima volta ha riconosciuto, con una storica decisione, un nuovo diritto costituzionale alla riservatezza ed integrità dei sistemi tecnologici d'informazione. [2] La prima questione che la Corte ha dovuto affrontare fu la costituzionalità di una legge che autorizzava i servizi segreti del Nord Reno-Westfalia a controllare ed investigare clandestinamente sulla rete Internet. In particolare, la legge avrebbe garantito ai servizi segreti il diritto di intercettare e cercare in modo occulto comunicazioni via Internet ed accedere segretamente ai sistemi tecnologici d'informazione. Tale legge era stata introdotta come emendamento all'articolo 5.2 n.11 della legge sulla protezione della costituzione nel Nord Reno-Westfalia dal Dicembre 2006.

La Corte nella sua decisione sostenne che queste attività investigative interferivano in realtà con diritti costituzionalmente garantiti. Quindi, qualsiasi legge che permetta attività simili deve essere in grado di dimostrare che tale intervento sia giustificato dalla protezione di altri diritti costituzionali, che lo stesso sia necessario per assicurare tale protezione e che sia proporzionato nel suo impatto. La Corte sostenne che la legge così come proposta non era conforme alla Costituzione e per questo illegittima.[3]

È stato largamente anticipato che la Corte avrebbe dichiarato incostituzionale l'emendamento.[4] Anche l'udienza preliminare prima della Corte costituzionale aveva già suggerito questo esito.[5] Tuttavia, il ragionamento della Corte e la portata della decisione furono una sorpresa per molti osservatori. Molti si aspettavano che la Corte avrebbe semplicemente esteso la sua ampia giurisprudenza riguardo la ricerca e i requisiti di confisca dei luoghi fisici del mondo online: invece, nella sua decisione, la Corte formulò un nuovo diritto fondamentale che protegge esplicitamente il diritto di Privacy e i diritti personali dei cittadini nelle Tecnologie dell'Informazione e Comunicazione (ICT).

2. *Premessa al caso*

L'oggetto della decisione era l'emendamento del paragrafo 5.2 della legge sulla protezione della Costituzione del Nord Reno-Westfalia dal Dicembre 2006. Ad ogni modo, l'emendamento di questa decisione era solo un aspetto nella discussione a livello federale riguardo la centralità di un nuovo metodo d'investigazione, la ricerca a distanza di computer e portatili. È quindi necessario tenere in conto questo precedente dibattito.

Il dibattito pubblico e giuridico su questo argomento si scatenò nel 2006 a partire da una richiesta operata da un procuratore statale alla Corte Federale di giustizia tedesca (Bundesgerichtshof, BGH). In questa domanda chiese un mandato per poter effettuare ricerche a distanza in computer sospetti nell'ambito di una investigazione sul terrorismo, istallando occultamente un programma di sorveglianza simile ad un Trojan. La richiesta venne rigettata il 25 novembre 2006. Il procuratore statale propose appello riferendosi agli artt. 102[6], 110[7] e 94[8] del codice penale i quali consentivano questo genere di ricerche. Nella sua argomentazione si supponeva una somiglianza sostanziale fra la ricerca fisica dei luoghi, regolata da questi articoli, e l'accesso a distanza di un computer di un sospettato. La BGH non era d'accordo, rigettando nel suo giudizio l'analogia tra una ricerca tradizionale di luoghi fisici e ricerche clandestine su computer.[9] Tuttavia, la decisione riguardava principalmente questioni formali di procedura, disponendo che senza un'esplicita regolamentazione, garantire una tale richiesta di autorizzazione sarebbe stato un atto *ultra vires*. La decisione lasciò aperta la possibilità che regolamentazioni appropriate avrebbero potuto essere introdotte per creare questa nuova ricerca e nuovi poteri di confisca: ciò ha evitato ogni decisione di merito sul potenziale conflitto che una legge potrebbe creare verso garanzie fondamentali della Costituzione. Lo stato del Nord Reno-Westfalia, modificando la legge già esistente per la protezione della Costituzione, creò un tale potere di diritto.

La legge sulla protezione della Costituzione nel Nord Reno-Westfalia dispone il diritto e stabilisce una base legale per le operazioni dell'Agenzia di protezione della Costituzione, i principali servizi segreti della Germania per gli affari internazionali. L'articolo 5.2 di questa legge definisce le azioni consentite per acquisire informazioni e dati privati dai sospettati. L'emendamento in questione dell'articolo 5.2 (11) della legge di protezione della Costituzione del Nord Reno-Westfalia, rinforzò l'Agenzia di protezione della Costituzione nell'eseguire due tipi di misure investigative: in primo luogo, il monitoraggio segreto e altre ricognizioni in Internet (Alternativa 1) e, in secondo luogo, l'accesso segreto ai sistemi tecnologici d'informazione (Alternativa 2). Il monitoraggio segreto di Internet è una misura con cui l'Agenzia di protezione della Costituzione ottiene informazioni sul contenuto di comunicazioni via Internet utilizzando le tecnologie di comunicazione nel modo consentito, come l'accesso ad un sito aperto, la partecipazione a chat o forum online, ma anche l'accesso a siti privati utilizzando una password ottenuta altrove, per esempio tramite un informatore.[10] Al contrario, l'accesso segreto ad un sistema tecnologico d'informazione è considerato un'infiltrazione tecnica, che può avvenire sfruttando falle nelle misure di sicurezza del sistema-bersaglio o tramite l'installazione di programmi-spia.[11]

Il metodo alla base della decisone, l'infiltrazione in un computer attraverso mezzi tecnici, riferito anche alla "ricerca online", "Trojan federali", o "ricerca a distanza", è una forma specifica di raccolta di informazioni. Tale metodo investigativo prova a risolvere le difficoltà nelle

investigazioni che emergono se criminali, in particolare gruppi terroristici, usano Internet per comunicazioni e per pianificare e commettere crimini.[12]

Lo scopo di setacciare un computer a distanza è quello di abilitare gli investigatori a cercare dei dati immagazzinati nell'hard disk e sulla memoria attiva del computer, intercettare il traffico di posta elettronica e controllare le abitudini di navigazione web e la messaggistica istantanea.[13] Per raggiungere tale scopo, un programma appositamente progettato, uno strumento "remote forensic software" (RFS), viene posto sul computer del sospettato senza che egli ne sia a conoscenza. Il programma è quindi in grado di copiare tutti i dati sul computer e successivamente trasferirli ai fini della valutazione. Un software di questo tipo condivide caratteristiche cruciali con dei malware ben conosciuti, in particolare virus e Trojan.[14] Questi ultimi in particolare possono essere usati per accedere al sistema-bersaglio ed estrarne dati personali, dunque sono adatti anche per la raccolta di dati da parte della polizia. Questo è il motivo per il quale l'RFS che facilita la ricerca a distanza in Germania viene spesso chiamato "Trojan federale". Il vantaggio nell'usare dette tecnologie è che possono essere istallate clandestinamente, senza entrare in casa del sospettato o in luoghi fisici. Gli strumenti RFS sono progettati per essere camuffati come programmi innocui quando in realtà includono un codice pericoloso e maligno, ingannando dunque il sospettato per indurlo ad installare il software. Quindi, come le loro controparti criminali, i Trojan della polizia richiedono la cooperazione ingenua del bersaglio.[15] Questo può accadere nell'aprire un'e-mail, per esempio un messaggio che si presume venire da una agenzia statale in buona fede, come il Consiglio locale o il Dipartimento delle pensioni.

Se l'infiltrazione riesce, questo metodo offre vantaggi considerevoli all'autorità investigativa rispetto ai metodi di investigazione tradizionali. Poiché tale metodo viene utilizzato all'insaputa del sospettato, costui non è allarmato dal fatto che la polizia lo consideri un obiettivo, in contrapposizione ad una tradizionale perquisizione in casa. Inoltre, il sistema consente la raccolta di dati criptati in forma decriptata potendo l'autorità investigativa accedervi nello stesso momento in cui l'utente li stia digitando. In aggiunta, possono essere raccolte password ed ulteriori informazioni sul modo di utilizzo del computer da parte del sospettato. Questo tipo di informazioni sarebbero difficili da ottenere utilizzando metodi investigativi tradizionali.[16]

Un ricorso costituzionale è ammesso dalla legge tedesca solo se il ricorrente può provare di essere direttamente colpito dall'atto statale e se uno dei diritti fondamentali elencati nella prima parte della Costituzione sia stato violato. L'emendamento del paragrafo 5.2 della legge sulla protezione della Costituzione del Nord Reno-Westfalia limita l'applicabilità di tale norma ad attività illegali "che minacciano il libero ordine fondamentale democratico o la sicurezza della Federazione o di uno stato Federale"[17], e durante la discussione riguardo l'introduzione della ricerca online come misura investigativa a livello federale è stato stabilito che questo potrebbe essere usato solo per indagare su sospettati in investigazioni sul terrorismo o casi comparabilmente gravi. Ciononostante, i quattro ricorrenti che depositarono un ricorso costituzionale contro l'emendamento del paragrafo 5.2 della legge sulla protezione della Costituzione nel Nord Reno-Westfalia affermarono che la norma costituiva una violazione diretta dei loro diritti costituzionali, anche se nessuno dei ricorrenti era stato coinvolto in indagini penali. La Corte accettò questo punto di vista ed ammise i ricorsi costituzionali. I quattro ricorrenti potevano tutti dimostrare che, sebbene non coinvolti loro stessi in alcun comportamento illecito, le loro attività professionali avrebbero potuto essere erroneamente classificate come tali, potendo così causare la perquisizione a distanza dei loro computer secondo il nuovo emendamento in violazione dei loro diritti garantiti dalla Costituzione. Uno di loro era un giornalista che accedeva a siti Internet gestiti da estremisti in connessione con organizzazioni eversive e che partecipava a chat ospitate in tali siti web, usando allo stesso tempo il computer per motivi privati. Un altro ricorrente era un membro di un partito politico sotto l'osservazione dell'Agenzia per la protezione della Costituzione del Nord Reno-Westfalia, che stava usando il computer sia per motivi di lavoro che per uso personale. Un ulteriore ricorrente era un avvocato che assisteva i richiedenti asilo, alcuni dei quali erano sotto il controllo dell'Autorità per la protezione della Costituzione del Nord Reno-Westfalia, utilizzando il computer allo stesso tempo per scopi di lavoro e privati.

Avendo superato il primo ostacolo ed avendo accettato una decisone di merito, ora la Corte doveva: (a) decidere se il paragrafo 5.2 della legge sulla protezione della costituzione del Nord Reno-Westfalia era costituzionale; e (b) considerare più in generare la costituzionalità di questo genere di metodi di investigazione.

3. *La decisione*

La Corte statuì che il paragrafo 5.2 della legge sulla protezione della Costituzione nel Nord Reno-Westfalia era non conforme alla Costituzione e pertanto nullo e privo di esecutività. Come già detto precedentemente, questo risultato non fu una sorpresa. Comunque, ciò che ci si aspettava era che la Corte per raggiungere questa conclusione si sarebbe limitata ad applicare i diritti fondamentali e i principi costituzionali esplicitamente enumerati. La Corte dispose che per varie ragioni il canone dei diritti esistenti non era sufficiente a proteggere le lesioni di diritti costituzionali che la ricerca a distanza di computer poteva causare. Questo creò – o forse venne dedotto dai primi principi – un nuovo diritto fondamentale alla riservatezza ed integrità dei sistemi tecnologici d'informazione.

Questa mossa a sorpresa era in parte dovuta al fatto ben accetto che la corte si impegnava in notevole profondità su specifiche questioni tecniche che la legge aveva sollevato. Tre dei principali esperti del mondo accademico in questo campo, Prof. Felix Freiling, della cattedra di Informatica dell'Università Mannheim, Prof. Dr. Andreas Pfitzmann, capo del gruppo di privacy e sicurezza dell'Università di tecnologie di Dresden e il Prof. Dr. Ulrich Sieber, direttore dell'Istituto per il diritto penale estero ed internazionale Max Plank, furono nominati in qualità di esperti tecnici della Corte. Forse più inusuale il passato di un quarto consulente della Corte, Andreas Bogk, collaboratore esterno in qualità di hacker al Clozure Inc e CEO del Chaos Computer Club Events, una delle più grandi ed influenti organizzazioni di hacker. La loro esperienza accademica e pratica fu profondamente compensata dalla Corte, di cui tutti i giudici (con una sola eccezione) precedentemente ricoprivano posizioni accademiche di alto livello.

3.1 *I ricorrenti*

Il Governo regionale del Lander del Nord Reno-Westfalia (avendo introdotto un nuovo potere investigativo) e il Governo Federale (in quanto partecipante alla questione nella Corte, ed anticipando un argomento simile a quello che si presentò successivamente per le Agenzie Federali) accettarono dall'inizio la necessità del rigido esame costituzionale della nuova misura. Tuttavia, argomentarono anche che gli strumenti RFS erano abbastanza simili al potere di polizia esistente nel mondo off-line e che l'applicazione analogica delle norme costituzionali pertinenti era sufficiente. Il Lander aggiunse inoltre che la legge come prevista era conforme alle relative previsioni della Costituzione. Nonostante questo fronte unitario sul principio, i due dichiaranti identificarono diverse norme costituzionali come "più vicine alla combinazione off-line". Il

Governo del Lander identificò il diritto costituzionale a garanzia della privacy nelle telecomunicazioni nell'articolo 10.1 della legge fondamentale tedesca (Gundgesetz – GG) come legge applicabile. Si discuteva se la ricerca on-line a distanza fosse essenzialmente una nuova forma di operazione di intercettazione e si propose una regolamentazione che estendesse la salvaguardia in vigore alle operazioni di intercettazione nelle nuove tecnologie. Il Governo Federale al contrario asserì che queste misure investigative sarebbero state coperte meglio dalla garanzia fondamentale dell'inviolabilità della dimora dell'articolo 13 GG, considerando le ricerche on-line come un equivalente alla ricerca fisica a casa di un sospettato.

Mentre c'era disaccordo sull'appropriata classificazione legale del procedimento delle ricerche a distanza, entrambe le parti erano concordi riguardo la regolamentazione dell'esito di tale ricerca. Ritennero che il diritto all'autodeterminazione dell'informazione come derivante dall'articolo 2.1 GG in connessione all'articolo 1.1 GG poteva servire da standard per una ricerca online. La discussione di diritto rispecchiò a questo proposito una precedente decisione della Corte Costituzionale che in passato aveva delineato la legge tedesca di protezione dati.

Secondo la posizione dello Stato e delle autorità investigative questa strategia aveva un senso. Potevano aver discusso sul fatto che le nuove tecnologie fossero così diverse dai poteri di polizia esistenti che nessuna delle norme costituzionali avrebbe trovato applicazione, e solo una legge incostituzionale come le previsioni di diritto penale contro l'hacking avrebbe necessitato di una modifica. Tuttavia, questa sarebbe stata una strategia ad alto rischio con scarse possibilità di successo. Era fin troppo ovvia la natura altamente intrusiva della tecnologia Remote Forensic Software (RFS) e fin troppo ovvie erano anche le somiglianze con sensibili forme di sorveglianza costituzionale per tentare di trattarla addirittura come un mero argomento di procedura di polizia. Ammettendo il punto principale, lo Stato era in grado di scegliere il suo campo di battaglia e di tratteggiare le decisioni rilevanti in maniera tale che le richieste di una conformità costituzionale non avrebbero distrutto l'efficienza della polizia. Le conseguenze di entrambi gli articoli per le procedure di polizia e pratica investigativa sono state ben comprese: un caso di diritto di notevole importanza crea un alto grado di certezza del diritto. Dato che una violazione della Costituzione potrebbe comportare l'inammissibilità di una prova altrimenti affidabile, un simile grado di certezza è altamente auspicabile per le pratiche di polizia. Volendo adottare una visione più cinica, si potrebbe dire che nel corso degli ultimi decenni polizia e servizi segreti hanno imparato a rispettare lo spirito di queste previsioni, lavorando in modo creativo al fine di aggirare le restrizioni. I codici che regolano le procedure di polizia e di investigazione penale, dei quali il più importante è la legge di procedura penale (Strafprozessordnung StPO) forniscono la procedura e le salvaguardie necessarie a concretizzare le norme a protezione della Costituzione. Gli ostacoli e i requisiti procedurali che la polizia deve osservare, per esempio i requisiti del mandato, differiscono nel dettaglio in caso di intercettazioni e ricerca in luoghi fisici. Non risulta chiaro perché il Governo Federale e statale abbiano espresso preferenze differenti. In generale, la posizione del Governo regionale era più violenta, la posizione del Governo federale più contenuta, poiché la protezione contro la perquisizione fisica è generalmente più rigorosa di quella delle operazioni di intercettazione. Concettualmente, i due approcci trattano una diversa cognizione della natura di Internet. Il Lander assunse un approccio conservatore che ridusse l'esperienza di Internet ai meri aspetti tecnici, cioè una comunicazione a distanza analoga ad una telefonata. Il Governo federale, al contrario, dimostrò la volontà di prendere in considerazione l'esperienza dell'utente e la sua conoscenza di complessi sistemi d'informazione, dunque concettualizzò alcune forme di utilizzo del computer e di Internet non solo come una banale attività radicata nel mondo fisico, ma come creazione a sé stante, un mondo digitale che merita di essere considerato più seriamente. La nostra "casa" è in parte online, pertanto le regole che proteggono le nostre dimore fisiche dovrebbero essere applicate anche ai nostri habitat digitali.

Nel prossimo paragrafo, analizzeremo come la Corte rispose a queste osservazioni.

3.2 ***Articolo 10.1 Grundgesetz – La segretezza delle telecomunicazioni***

Il diritto alla segretezza delle comunicazioni a distanza secondo l'Articolo 10.1 GG protegge le trasmissioni non fisiche di informazioni ad individui riceventi con l'ausilio di dispositivi di telecomunicazione:[18]

1. *La riservatezza della corrispondenza, della posta e delle telecomunicazioni è inviolabile.*
2. *Le restrizioni possono essere ordinate solo in virtù della legge. Se la restrizione serve a proteggere il libero ordine democratico fondamentale o l'esistenza o la sicurezza della Federazione o del Lander, la legge può prevedere che la persona interessata non debba essere informata della restrizione e che il ricorso ai tribunali venga sostituito da una revisione del caso da parte di agenzie e agenzie ausiliarie nominate dal legislatore.*

La protezione di questo diritto fondamentale copre ogni tipo di telecomunicazione indipendentemente dal tipo di trasmissione utilizzata (via cavo o radiotrasmissione, trasmissione analogica o digitale) e i dati trasmessi (discorsi, immagini, suoni, o altre informazioni). Lo scopo della protezione della segretezza delle telecomunicazioni pertanto include anche qualsiasi comunicazione a distanza via Internet.[19] Inoltre, questa legge non protegge solo i contenuti delle comunicazioni a distanza, ma anche i dettagli più generali, come l'identità di chi comunica e il tipo di trasmissione (tramite e-mail, chat, o VoIP).[20] Inoltre, fatto particolarmente importante per il contesto online, i metadati generati come risultato di comunicazioni sono stati inclusi nell'ambito dell'articolo da precedenti decisioni dei tribunali. La Corte inoltre affermò che ogni continua comunicazione via Internet e i dati generati da tali comunicazioni cadono nell'ambito dello scopo della protezione dell'articolo 10.2 GG. Quindi, ogni metodo di indagine fondato sulle comunicazioni in corso ed i dati da esso emersi devono risultare in conformi al diritto alla segretezza delle telecomunicazioni di cui all'articolo 10.1 GG. Il campo di applicazione della protezione di questo diritto fondamentale prescinde dal fatto che la misura riguardi il canale di trasmissione o il terminale utilizzato per la telecomunicazione.[21]

Come visto precedentemente, l'art. 10(2) GG permette l'intercettazione di comunicazioni a certe condizioni e il Governo del Lander del Nord Reno-Westfalia ha affermato che l'emendamento del paragrafo 5.2 della legge sulla protezione della Costituzione nel Nord Reno-Westfalia soddisfa i requisiti costituzionali come la giustificazione dell'intrusione.[22] Secondo la procedura, è necessario che una legge crei i poteri di polizia pertinenti. Nella sostanza, qualsiasi legge che violi *prima facie* un diritto costituzionale deve avere come scopo la protezione di un altro diritto elencato nella Costituzione, la violazione del diritto deve essere necessario a raggiungere l'obiettivo previsto e la violazione deve essere proporzionata alla protezione che si ottiene.[23] Il modo in cui la legislazione raggiunga questo giusto equilibrio è comunque affidato alla discrezionalità del Parlamento. A titolo puramente esemplificativo, prevedere un requisito per i mandati giudiziari in tale normativa aiuterebbe a passare il test di costituzionalità, ma non è un requisito costituzionale diretto. Concettualizzare la sorveglianza on-line per mezzo di Trojan, come l'intercettazione della comunicazione, è stato il punto di vista proposto dal Governo del Nord Reno-Westfalia e dalle forze di polizia, basato sull'idea che lo stesso Trojan funziona solo quando c'è una connessione attiva della comunicazione, cioè quando il

computer è connesso ad Internet e i dati vengono trasmessi.

La Corte concordò solo in parte con questa analisi. Constatò in particolare che l'articolo 10.1 GG non protegge i dati delle telecomunicazioni, che sono memorizzati su dispositivi ICT dopo che il corso della comunicazione è completato, soprattutto se le informazioni non sono di dominio pubblico e la persona interessata abbia intrapreso misure per proteggere i dati da accessi non autorizzati.[24] Inoltre, la Corte ha dichiarato che la protezione dell'articolo 10.1 GG non si applica se un ente di stato controlla l'utilizzo di un sistema tecnologico di informazione in quanto tale o effettua ricerche negli archivi del sistema. Questo è anche il caso in cui una connessione di telecomunicazione venga usata per trasmissioni di dati raccolti da un'autorità di valutazione, come è il caso per esempio della ricerca on-line di computer.[25] A nostro avviso, questa analisi è corretta. Che il Trojan richieda che ad un certo punto il sospettato sia on-line e sia impegnato nella comunicazione non rende la ricerca un'operazione di intercettazione più di quanto un ufficiale di polizia che si impossessi del telefono dei sospettati nel corso di una perquisizione fisica dei locali possa cambiare la natura dell'operazione da una perquisizione ad una intercettazione di comunicazioni a distanza.

L'infiltrazione segreta in un complicato sistema tecnologico di informazione offre l'opportunità di spiare il sistema nel suo complesso e non è solo un'intercettazione di uno scambio isolato di comunicazioni come in una tradizionale operazione di intercettazione.[26] In particolare, c'è la possibilità che i dati personali memorizzati nel computer, che sono estranei e vanno oltre il contenuto e le circostanze relative al corso della comunicazione a distanza, vengano raccolti (anche se questo avviene involontariamente). Così, la potenziale minaccia contro le libertà civili va ben al di là della mera sorveglianza delle telecomunicazioni e anche al di là della portata della tutela dell'articolo 10.1 GG.

La Corte pertanto arrivò alla conclusione che l'articolo 10.1 GG può solo fornire protezione sufficiente contro le infiltrazioni in un sistema tecnologico di informazione se la sorveglianza è ristretta esclusivamente a dati provenienti da una telecomunicazione in corso.[27] Se l'infiltrazione serve a raccogliere dati, ad esempio copiandoli dagli hard drive, l'articolo 10.1 GG non è richiamabile. In pratica, difficilmente ogni ricerca sarà considerabile una "pura" intercettazione di comunicazioni. Il principale scopo degli strumenti RFS come esposto in precedenza è raccogliere dati memorizzati in un computer e il divario concettuale con l'intercettazione di una comunicazione è troppo ampio per essere colmato tramite un'interpretazione analogica dell'articolo 10.1. Questo vuol dire anche che molti aspetti della ricerca a distanza di computer non sono coperti dalla garanzia della segretezza nelle telecomunicazioni come previsto dall'articolo 10.1 GG.

3.3 *L'articolo 13.1 Grundgesetz – L'inviolabilità della dimora*

La garanzia dell'inviolabilità della dimora previsto all'articolo 13.1 GG protegge lo spazio della vita privata dalle intrusioni dello stato:

1. *La dimora è inviolabile.*

Questo garantisce agli individui uno spazio essenziale come una condizione necessaria per la dignità personale, nonché nell'interesse dello sviluppo delle loro personalità. Detta garanzia può essere limitata solo in condizioni particolari come indicato dall'articolo 13.2 al 13.7 GG:

2. *Le ricerche possono essere autorizzate solo da un giudice o, quando il tempo è essenziale, da altri autorizzati designati dalla legge, e possono essere effettuate solo nei modi in questa prescritti.*

3. *Se fatti particolari giustificano il sospetto che una persona abbia commesso un crimine particolarmente grave specificamente definito da una legge, mezzi tecnici di sorveglianza acustica di ogni casa in cui l'indagato si suppone soggiornare possono essere impiegati ai sensi del provvedimento giudiziario al fine di perseguire il reato, a condizione che metodi alternativi per indagare sulla questione sarebbero sproporzionatamente difficili o improduttivi. L'autorizzazione deve essere concessa per un tempo determinato. L'ordine deve essere rilasciato da una giuria composta da tre giudici. Quando il tempo è essenziale, può anche essere emesso da un giudice unico.*

4. Per prevenire gravi pericoli per la sicurezza pubblica, in particolare i pericoli contro la vita o la società, mezzi tecnici di sorveglianza della dimora possono essere impiegati solo in virtù di un provvedimento giudiziario. Quando il tempo è essenziale, tali misure possono anche essere ordinate da altre autorità designate dalla legge; una decisione giudiziaria dovrà essere successivamente ottenuta senza ritardo.

5. Se i mezzi tecnici sono contemplati esclusivamente per la protezione di persone ufficialmente presenti in una casa, la misura può essere ordinata da un'autorità designata dalla legge. Le informazioni così ottenute possono essere altrimenti usate solo al fine di un procedimento penale o per prevenire pericoli e solo se la legittimità del provvedimento sia stata precedentemente determinata da un giudice; quando il tempo è essenziale, una decisione giudiziaria dovrà essere successivamente ottenuta senza ritardo.

6. Il Governo Federale dovrà riferirsi annualmente al Bundestag per l'impiego dei mezzi tecnici ai sensi del paragrafo (3) e, nell'ambito della giurisdizione della Federazione, ai sensi del paragrafo (4) e, nella misura in cui è richiesta l'approvazione giudiziaria, ai sensi del paragrafo (5) del presente articolo. Una commissione eletta dal Bundestag eserciterà il controllo parlamentare sulla base di questa relazione. Un controllo parlamentare analogo dovrà essere accordato dal Lander.

7. Interferenze e restrizioni potranno altrimenti essere permesse solo per prevenire un pericolo della società o della vita di un individuo, o, in virtù di una legge, per affrontare un pericolo grave per la sicurezza e l'ordine pubblico, in particolare per risolvere una carenza di alloggi, per combattere il pericolo di un'epidemia, o per proteggere i giovani da un rischio.

La sfera spaziale in cui la vita privata si svolge costituisce l'interesse protetto da tale diritto fondamentale.[28] Lo spazio della vita privata, tuttavia, non è limitato all'appartamento privato o alla casa degli aventi diritto, ma include anche il luogo degli affari e di lavoro.[29] Questo spazio è protetto da intrusioni fisiche, nonché dall'uso di misure tecniche che forniscano una visione degli avvenimenti altrimenti protetti all'interno dello spazio della vita privata. Si tratta, ad esempio, della sorveglianza acustica e visiva di un luogo abitato,[30] ma anche di controlli effettuati con radiazioni elettromagnetiche finalizzati a monitorare l'utilizzo di sistemi tecnologici di informazione all'interno dell'abitazione.

Il Governo Federale ha sostenuto che la ricerca on-line su computer può essere comparata alla ricerca in abitazione, e l'articolo 13 GG può pertanto essere usato come standard per tali misure. Come abbiamo visto, a differenza delle precedenti disposizioni, l'articolo 13 contiene delle condizioni direttamente ed esplicitamente non negoziabili per ogni infrazione prima facie. Questo significa che lo Stato è notevolmente più limitato nell'adeguare il relativo diritto processuale per accogliere le nuove tecnologie. Mentre non c'è una classifica ufficiale fra i differenti diritti costituzionali, la maggior cura che gli autori hanno utilizzato per specificare in alcuni dettagli il nucleo non negoziabile di cui

all'articolo 13 nel rispetto dell'articolo 10, indica quanto gravi vengano considerate le interferenze nello spazio fisico. Conseguentemente, il Governo Federale ammise che l'alta "intensità" di una invasione nelle libertà civili che ogni restrizione dell'articolo 13 porta vuol dire anche che tali misure dovrebbero essere sempre e solo un'ultima ratio per una Agenzia (federale e statale) di protezione della Costituzione.

Come con l'analisi svolta sull'articolo 10, la Corte ha in parte condiviso ed in parte respinto questo esame. Constatò che l'articolo 14.1 GG potrebbe solo fornire protezione allo spazio della vita privata, sia contro le intrusioni segrete da parte della polizia o dei servizi segreti finalizzate a manipolare fisicamente i sistemi tecnologici di informazione, sia contro le infiltrazioni di tali sistemi per monitorare gli eventi in un appartamento con una periferica collegata (come ad esempio l'utilizzo di microfoni installati per le intercettazioni).[31]

Fu stabilito che tali azioni avrebbero dovuto essere comparabili per loro natura alla ricerca tradizionale in un'abitazione e pertanto essere coperte dall'articolo 13 GG. Tuttavia, anche tale protezione non fece molta strada, sottovalutando l'importanza del mondo digitale per i cittadini di oggi. La Corte dichiarò che l'articolo 13 GG non è sufficiente a proteggere i diritti dei titolari contro un'intrusione nei sistemi tecnologici di informazione utilizzando un Trojan o software simili per accedere ai dati memorizzati e per monitorare le comunicazioni, anche se il sistema è situato in una casa.[32] Un problema specifico creato dalle ricerche RFS è che le intrusioni e il monitoraggio possono essere eseguite a prescindere dal luogo dove è situato sistema tecnologico di informazione. Quindi, una protezione dipendente dal luogo è inutile se il sistema si trova al di fuori dello spazio privato o in movimento tra aree protette. In particolare, i piccoli dispositivi tecnologici come portatili, PDA e telefoni cellulari sono progettati per essere trasportati. La precisa posizione del sistema è spesso sconosciuta, oltre ad essere irrilevante per gli investigatori nel caso di infiltrazione nel dispositivo di accesso ai dati memorizzati. Questo avrebbe comportato la paradossale conseguenza che un cittadino che inizi a scrivere un'e-mail sul suo computer portatile a casa e la riesamini su una panchina del parco completandola e rimandandola a casa si muova tra ambienti protetti e non protetti, perdendo e guadagnando la protezione costituzionale, creando quindi distinzioni artificiali in un'attività percepita da parte del cittadino come uniforme.

3.4 *Articolo 2.1 Grundgesetz in combinato disposto con l'articolo 1.1 Grundgesetz - Il diritto all'autodeterminazione dell'informazione*

Dopo aver analizzato e respinto in quanto insufficienti sia l'articolo 10 che l'articolo 13, la Corte ha sviluppato la propria risposta. Ha iniziato la sua analisi con l'intuizione ormai comune che, a causa dei recenti sviluppi tecnologici, i sistemi di informazione sono onnipresenti nella società di oggi e il loro utilizzo è di grande importanza per molti cittadini.[33] Questo vale in primo luogo per i personal computer ma, come sottolinea la Corte, l'importanza dei dispositivi tecnologici non si limita solo ad essi. Riconobbe che molti oggetti che vengono utilizzati quotidianamente dalla popolazione tedesca comprendono elementi di tecnologia dell'informazione.[34] Telefoni cellulari, BlackBerry e anche lettori MP3 sono esempi importanti di dispositivi di uso frequente. Inoltre, frigoriferi automatici, tostapane e anche gioielli stanno già comparendo all'orizzonte come prossime estensioni. La Corte riconobbe poi che il significato culturale e sociale di tali dispositivi e dei personal computer in particolare è cresciuto significativamente, in quanto possono essere utilizzati per una vasta gamma di motivi, come la completa amministrazione e l'archiviazione di questioni private, di affari o per intrattenimento nel tempo libero.[35] In tal modo, i dati memorizzati sui dispositivi tecnologici di informazione forniscono informazioni globali sulle circostanze personali, contatti sociali, preferenze individuali e le attività degli utenti.

La Corte sostenne che per la maggior parte delle persone, l'uso di Internet è una parte essenziale del modo in cui esse vivono le loro vite ed è un aspetto importante del modo in cui si sviluppa e si esprime la propria personalità. Affermò anche che la crescente diffusione di dispositivi di informazione e la dipendenza da essi crea nuovi pericoli per lo sviluppo personale degli individui. In aggiunta ai dati potenzialmente sensibili memorizzati sugli stessi dispositivi, l'utente di un dispositivo connesso ad Internet lascerà (consapevolmente o inconsapevolmente) dati ed informazioni relative alla sua personalità e al comportamento degli utenti su vari server. La conoscenza di ogni singola parte di tali dati può essere innocua ma, come la Corte ha sostenuto, la combinazione dei dati memorizzati su dispositivi detenuti da altri soggetti in una rete può rendere possibile la formazione di un profilo, se una terza parte li raccoglie e li valuta.[36] Soprattutto, però, la messa in rete del sistema apre a terzi una struttura tecnica di accesso, che può essere usata per spiare o manipolare i dati ivi conservati. L'individuo talvolta non è in grado di rilevare tale accesso o può perlomeno solo evitarlo in misura limitata.[37]

La combinazione tra la modifica del significato sociale e culturale dell'uso di dispositivi di informazione per lo sviluppo della propria personalità ed il riconoscimento di nuove minacce al libero sviluppo dell'individualità, come nuove capacità di prelevamento di dati, ha portato il giudice a riconoscere l'importanza fondamentale della solidificazione di garanzie costituzionali nell'ambiente on-line.

Nell'anno in cui la prima wide-area network basata su TCP/IP divenne operativa e tutti gli host su ARPANET smisero di utilizzare protocolli NCP, cinque anni prima dell'apertura di Internet a provider commerciali, la Corte Costituzionale in una decisione storica non collegata all'ICT aveva creato il nucleo della legge tedesca sulla protezione dei dati.[38] Il diritto all'autodeterminazione dell'informazione, che non viene menzionato esplicitamente dalla Costituzione, era derivato dall'articolo 2.1 in combinato disposto con l'articolo 1.1 GG, i quali garantiscono il diritto al libero sviluppo della propria personalità ed il generale "diritto alla dignità". Pronunciandosi sulla costituzionalità del censimento nazionale, stabilì un diritto legale alla capacità dell'individuo di determinare in linea di principio la divulgazione e l'uso dei propri dati personali.[39] Questo diritto risultò dal riconoscimento da parte della Corte che lo Stato può effettuare molteplici processi di raccolta e di utilizzo di dati privati e che l'evoluzione del data processing le ha semplificate a tal punto che è diventato possibile ottenere un'immagine dettagliata della personalità di un individuo. Ciò aveva il potenziale per nuocere gli interessi alla riservatezza della persona interessata, i quali sono protetti dai diritti fondamentali. Inoltre, la mera previsione che i propri dati possano essere raccolti comportò una lesione inaccettabile della propria libertà di condotta, incoraggiando le persone ad una valida, e perfettamente legale, rinuncia di scelte di vita nella mera previsione che le informazioni su di loro avrebbero potuto essere raccolte e comunicate a terzi. Inoltre, alcune minacce possono essere non percepibili. La Corte affermò che ciò avviene quando dati personali sono usati e collegati con modalità che il titolare non può individuare né impedire.[40] La paura della sorveglianza è come la sorveglianza stessa: un limite al libero sviluppo della personalità sociale.

Sia il Governo del Lander del Nord Reno-Westfalia che il Governo Federale ammisero che il diritto all'autodeterminazione dell'informazione dovrebbe essere uno standard di diritto fondamentale per le ricerche on-line, ma sostennero anche che lo stesso è sufficiente per regolare le misure investigative.

Tuttavia, la Corte ha rilevato che il diritto all'autodeterminazione dell'informazione non considerava sufficientemente il fatto che le persone si affidano ai sistemi informatici per sviluppare la loro personalità e conferiscono al sistema dati sensibili, o forniscono tali dati semplicemente

utilizzando il sistema.[41] Un terzo che acceda ad un simile sistema può potenzialmente ottenere una grande quantità di dati sensibili riguardo un individuo, senza dover ricorrere ad un'ulteriore raccolta di dati e misure di elaborazione. In un certo senso, si potrebbe dire che queste misure 'cut out the middle man': i dati vengono già elaborati ed organizzati dalla persona interessata. Poiché la precedente decisione sulla protezione dei dati si incentrò sul processo di trattamento dei dati e sull'organizzazione, rischiava di essere aggirata con la nuova tecnologia di sorveglianza. L'inconsapevole partecipazione attiva del sospettato, fondamentale per il funzionamento dell'RFS, ha quindi anche il potenziale di impedire all'indagato di ottenere in altro modo la protezione a lui riconosciuta. La ricerca on-line su computer è una minaccia per la personalità dell'interessato: poiché va oltre la semplice raccolta di dati personali, contro la quale il diritto all'autodeterminazione dell'informazione fornisce protezione, non rientra nella tutela di questo diritto fondamentale.

4. *Il diritto alla riservatezza ed integrità dei sistemi tecnologici di informazione*

Avendo stabilito che i diritti esistenti non sono sufficienti per proteggere i cittadini dalla minacce contro i loro diritti della personalità, la Corte stabilì un nuovo diritto fondamentale alla riservatezza ed integrità dei sistemi tecnologici di informazione per colmare così la lacuna normativa.

Come il diritto fondamentale all'autodeterminazione dell'informazione, questo diritto non è esplicitamente menzionato nella Costituzione. Sebbene non avvenga molto spesso in Germania che un nuovo diritto fondamentale sia stabilito per mezzo di un attivismo giudiziario, il potere della Corte a colmare creativamente le lacune individuate nel quadro dei diritti civili previsti dalla Costituzione è ampiamente riconosciuto e, a differenza degli Stati Uniti, il c.d. 'originalism' non ha mai rappresentato una posizione di rilievo nella Germania del dopoguerra.[42]

Così come il diritto all'autodeterminazione dell'informazione, questo nuovo diritto fondamentale si basa sull'articolo 2.1 GG in combinato disposto con l'articolo 1.1 GG ed è derivato da un generale diritto della personalità. L'articolo 1 GG, il quale dispone che "la dignità umana è inviolabile, e tutti gli organi dello stato hanno l'obiettivo finale di proteggerla" stabilisce un generale principio fondamentale nel sistema legale tedesco ed è stato progettato esplicitamente come soluzione per eliminare le lacune se le soluzioni legislative non rispettano il cambiamento sociale. Il nuovo diritto costituzionale alla segretezza ed integrità dei sistemi tecnologici di informazione, secondo la Corte, protegge la vita personale e privata dei titolari dei diritti dall'accesso statale a dispositivi tecnologici di informazione, in particolare dall'accesso da parte dello Stato ai sistemi tecnologici di informazione nel loro complesso, non solo dunque per eventi di comunicazione individuale o memorizzazione dei dati.[43]

4.1 *Quali sistemi sono protetti?*

La Corte applica le garanzie di questo diritto ai sistemi tecnologici di informazione, ma è interessante notare che così facendo non fornisce una definizione di tale sistema. Invece, elenca i sistemi che non sono protetti da questo diritto e fornisce una descrizione delle capacità minime che un sistema tecnologico informatico deve possedere per rientrare nel campo di applicazione della tutela di questo diritto fondamentale. Così facendo, mantiene molto ampia la portata della protezione del diritto e volutamente evita il riferimento a tecnologie specifiche. In tal modo, riconosce chiaramente la rapida evoluzione tecnologica dei dispositivi tecnologici di informazione e con la sentenza in esame tenta di creare una normativa neutrale per la tecnologia, cercando quindi di mantenere il nuovo diritto fondamentale "a prova di futuro".[44]

La Corte rileva che non tutti i sistemi che siano in grado di creare, elaborare o immagazzinare dati personali richiedono una speciale protezione di una garanzia separata dei diritti personali.[45] I sistemi che contengono dati pertinenti solo ad un certo aspetto della vita della persona interessata non sono protetti da questo nuovo diritto fondamentale. Tali sistemi potrebbero essere, ad esempio, sistemi di controllo elettronico non in rete degli elettrodomestici.[46] Certamente, l'accesso a tali dati non consentirebbe alle autorità di acquisire una visione dettagliata della personalità dell'interessato.

L'ambito di protezione del diritto fondamentale alla riservatezza ed integrità del sistema tecnologico di informazione è applicato a sistemi che da soli, o nella loro interconnessione, possano contenere dati personali dell'interessato tali che l'accesso al sistema faciliti la penetrazione in parti significative della sua vita o mostri un'immagine rivelatrice della sua personalità.[47] Detti sistemi sono ad esempio personal computer e computer portatili (utilizzati sia per motivi privati che di lavoro) o telefoni cellulari ed agende elettroniche, le quali hanno un gran numero di funzioni e possono raccogliere e memorizzare molti tipi di informazioni personali. È interessante notare che la Corte decise che la mera *capacità* di un sistema di memorizzare dati personali sia sufficiente. Se questa capacità sia o meno utilizzata dall'utente non deve essere determinato nel singolo caso. Ciò vuol dire che tale diritto protegge un sistema, come ad esempio un computer, anche se non contiene realmente dati sensibili personali, fintanto che sia tecnicamente in grado di memorizzare ed elaborare tali informazioni. Inoltre, si ritiene che i sistemi che fanno parte di una rete (come Internet) non sempre contengono dati personali di per sé, ma i dati sulla persona in questione possono essere memorizzati su un altro sistema all'interno della rete che, se penetrato, può rendere i dati accessibili a terzi. Questo nuovo diritto fondamentale è pertanto da applicare a dati che siano posti in outsourcing, ad esempio utilizzando una tecnologia cloud computing.[48] Ciò rende la decisione anche la prima che abbia esplicitamente riconosciuto una delle questioni giuridiche che il cloud computing e la sua diffusione inevitabilmente genereranno.

4.2 *Cosa è protetto?*

Cosa precisamente protegge il diritto fondamentale all'integrità e segretezza dell'informazione dei sistemi tecnologici? In primo luogo, protegge l'interesse degli utenti di un sistema tecnologico di informazione a che i dati creati, trattati e memorizzati dal sistema rimangano riservati.[49] In secondo luogo, il diritto è violato se l'integrità di un sistema sia minacciata da terzi che possano usare le sue potenzialità, funzioni e contenuti della memoria. Questo significherebbe, come stabilisce la Corte, che l'ostacolo tecnico maggiormente critico per consentire lo spionaggio, la sorveglianza o la manipolazione del sistema dovrebbe essere superato.[50]

La Corte ha specificato inoltre che tale diritto fondamentale protegge il titolare del diritto in particolare dall'accesso occulto ad un sistema tecnologico di informazione che si rivolga al sistema nel suo complesso o alla sua parte più importante. L'ambito della protezione offerta da questo diritto copre sia la conservazione dei dati sulla memoria di lavoro nonché i dati che siano temporaneamente o permanentemente conservati sul supporto di memoria del sistema. Protegge anche dall'acquisizione di dati che non si avvalga delle procedure di elaborazione del sistema stesso ma che abbia questi obiettivi, come ad esempio i cosiddetti key-logger, che controllano i tasti di un utente per ottenere password ed altri importanti dati di log-in.[51]

Inoltre, la Corte stabilisce che la tutela derivante da questo diritto fondamentale non dipende dal grado di difficoltà di accesso al sistema. Riconosce quindi che gli utenti dei sistemi tecnologici di informazione hanno una varia conoscenza dei mezzi tecnici per proteggere i sistemi dalle intrusioni e non concede agli utenti con una migliore conoscenza un più elevato grado di protezione.

Tuttavia, una protezione sussiste solo se un soggetto interessato considera il sistema come di sua proprietà e quindi possa presumere che solo lui o altri soggetti da lui autorizzati, come i membri della famiglia, lo usino in modo auto-determinato. L'uso di un accesso pubblico ad un sistema tecnologico di informazione in una stazione ferroviaria che fornisca orari ed informazioni di viaggio non è quindi coperto. Tuttavia è anche coperto l'uso di una propria rete tramite l'utilizzo di sistemi tecnologici di informazione che siano a disposizione degli altri. Ad esempio questo potrebbe avvenire nel caso dell'accesso a distanza del proprio sistema o di un dispositivo esterno di memorizzazione attraverso un computer in un Internet Point.

4.3 ***Le restrizioni***

Ad ogni modo, il diritto alla segretezza ed integrità dei sistemi tecnologici di informazione non è assoluto. Può essere limitato sia per motivi di prevenzione che per perseguire crimini. Tuttavia, qualsiasi misura che limiti questo diritto fondamentale deve essere proporzionata alla violazione, soprattutto se la misura è eseguita senza la conoscenza del sospettato. Quindi, la Corte ha rilevato che una misura che limiti questo diritto sia proporzionata solo ove esistano prove sufficienti che significativi valori fondamentali di rango superiore debbano essere protetti. Valori fondamentali di rango superiore sono la vita e l'integrità degli altri cittadini, i fondamenti dello Stato e i valori essenziali di umanità.[52] Tuttavia, la Corte successivamente mitiga questo requisito statuendo che non è richiesto un alto grado di probabilità che un pericolo si verifichi in un prossimo futuro.[53]

Per di più, ognuna di queste misure deve essere esaminata e confermata da un giudice con una decisione caso per caso per garantire un controllo oggettivo ed indipendente prima dell'esecuzione, e questo deve trovare fondamento in una base giuridica costituzionale.[54]

Un requisito ulteriore è che ogni misura restrittiva del diritto alla segretezza ed integrità dei sistemi tecnologici di informazione non violi l'area centrale della gestione privata della vita, la quale include fra le altre cose la comunicazione e l'informazione a proposito di sentimenti intimi e profonde relazioni. La conduzione privata della vita è un diritto fondamentale assoluto, il quale non può essere ristretto (articolo 1.1 GG – diritto alla dignità umana). Dal momento che sarà spesso molto difficile distinguere tra l'area centrale e quella non centrale dei dati durante il processo di indagine, la Corte afferma che le procedure adeguate devono essere in vigore per la fase dell'esame dei dati. In particolare, se l'area centrale dei dati è individuata immediatamente, tali informazioni devono essere subito cancellate e l'utilizzo delle stesse da parte dello Stato è proibito.[55] Comunque, questo fa sorgere il dilemma se la richiesta di cancellazione dell'area centrale dei dati raccolta non possa annullare la violazione del diritto assoluto alla dignità umana. Inoltre, come sottolinea Kutscha, sebbene la misura stessa debba essere permessa dal giudice, la Corte non può stabilire una richiesta al giudice per controllare il processo di analisi.[56]

5. ***Conclusioni***

Il ragionamento della Corte è stato, dal punto di vista della tecnologia o da una prospettiva tecnologicamente consapevole, eccezionalmente ben fondato, opponendosi in tal modo a chi critica sostenendo che le risposte giuridiche siano spesso formulate da persone incompetenti in ambito tecnico. Inoltre, il diritto fondamentale di nuova concezione è stato elaborato in modo sufficientemente ampio, abbastanza da poter affrontare i futuri sviluppi tecnologici.

Mentre l'impulso principale del Governo era quello di aumentare la protezione dei cittadini, la Corte ha stabilito che la ricerca on-line a distanza nei computer non è in genere una misura incostituzionale, ma che la normativa che la consente dovrà essere in stretta conformità con il diritto alla riservatezza e all'integrità dei sistemi tecnologici di informazione in aggiunta alla protezione già affermata dagli articoli 10 e 13 GG. Da un lato, questo significa che la Corte ha spianato la strada alla Germania per agire secondo la raccomandazione del Consiglio dell'Unione Europea, secondo la quale gli Stati Membri dovrebbero facilitare la ricerca segreta dei computer dei sospettati per combattere la criminalità informatica.[57] Allo stesso tempo, ha stabilito notevoli ostacoli procedurali per l'uso di questa tecnologia. Un problema che non può essere affrontato in questo documento è il potenziale conflitto di frontiera che la tecnologia potrebbe comportare se un RFS migrasse al di fuori della giurisdizione della polizia inquirente o se i sospettati portassero fisicamente all'estero un dispositivo "infetto".[58] Poiché la protezione di cui all'articolo 1 copre anche i cittadini stranieri sul territorio tedesco, il potenziale del conflitto è quindi elevato se altri stati membri decidessero di introdurre la tecnologia con garanzie comparativamente più basse.

Con la formulazione del nuovo diritto fondamentale alla segretezza ed integrità dei sistemi informatici, la Corte, per la prima volta, ha riconosciuto che le tecnologie non svolgono solo un ruolo importante nella vita delle persone come un'aggiunta o un'estensione al vivere nel mondo fisico, ma anche che un numero crescente di persone vive "in linea". Internet è diventato uno spazio di vita, dove le persone incontrano amici, formano società e scambiano informazioni, e la Corte ha riconosciuto che la normativa esistente non è sufficiente a proteggere adeguatamente i cittadini dalle violazioni da parte dello stato di questo ambiente digitale. Il "cittadino digitale", come risultato di questo caso, ha fatto un passo in avanti. Per la stessa ragione, non si può escludere che in futuro la Corte estenderà questo concetto anche nella direzione opposta. Attualmente, il Trojan federale è inteso come uno strumento digitale utilizzato da ufficiali di polizia in carne ed ossa. Ma se la Corte prende il proprio ragionamento sul serio, lo stesso Trojan si potrebbe anche considerare come un "ufficiale di polizia digitale", soggetto alle stesse restrizioni, ma anche agli stessi poteri che la sua controparte fisica possiede. È probabile che si verificheranno in futuro nuovi tentativi, da parte dei Governi regionali e federali in Germania, di creare leggi procedurali "a prova di costituzione" che prevengano il preciso fondamento giuridico richiesto dalla Corte. È probabile che vedremo sfide contro leggi riformulate seguendo l'esempio, dando alla Corte possibilità in più di approfondire il nuovo diritto alla riservatezza ed integrità dei sistemi informatici. In particolare, "l'effetto sui terzi" della sentenza non è ancora stato determinato, così come il grado con cui i datori di lavoro, ISP e content provider, come ad esempio Google, saranno considerati potenziali trasgressori di questo nuovo diritto. La vicenda UK Phorm, ad esempio, sembra un'applicazione ideale di tale diritto agli attori del settore privato. Questo richiederà anche di ripensare alla puntuale relazione tra il nuovo diritto e il suo fratello maggiore, il diritto all'autodeterminazione dell'informazione. L'autodeterminazione dell'informazione, come suggerisce la parola stessa, riguarda innanzitutto le libere scelte degli interessati, compresa quella di poter condividere o meno i propri dati. Tale elemento di scelta è assente nel nuovo diritto e ciò fa sorgere ancora più dubbi sull'eventualità che l'attuale prassi di richiedere il consenso da parte dei gestori di dati possa essere in futuro considerata sufficiente.

---

[1] In seguito "La Corte".

[2] BVerfG, NJW 2008, 822.

[3] Ibid.

[4] Vedi es., G. Hornung, "Ein neues Grundrecht. Der verfassungsrechtliche Schutz der "Vertraulichkeit und Integritat informationstechnischer Systeme"", (2008) 5 *Computer und Recht*, 299.

[5] M. Kutscha, "Mehr Schutz von Computerdaten durch ein neues Grundrecht?", (2008) 15 *Neue Juristische Wochernschrift*, 1042-1044.

[6] Regola la ricerca dei locali.

[7] Regola la confisca e la ricerca di documenti e di dispositivi di memoria digitali.

[8] Regola la salvaguardia e la confisca delle prove.

[9] BGH, NJW 2007, 930.

[10] BVerfG, NJW 2008, 822 (825).

[11] Ibid.

[12] BVerfG, NJW 2008, 822 (826).

[13] K. Leipold, "Die Online-Durchsuchung", (2007) 4 *Neue Jurisstische Wochenschrift Spezial* 135.

[14] U. Buermeyer, "Die 'Online-Durchsuchung' – Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", (2007) 4 *Hochstrichterliche Rechtrprechug im Strafrecht* 154.

[15] Ibid.

[16] BVerfG, NJW 2008, 822 (826).

[17] Par. 3.1 Verfassungsschutzgesetz Nordrhein-Westfalen.

[18] Vedi ad es. BVerfGE 67, 157 (172); 106, 28 (35).

[19] Vedi BVerfGE 113, 348 (383) per le e-mail.

[20] Vedi ad es. BVerfGE 67, 157 (172); 85, 386 (396).

[21] BVerfGE 106, 28 (37-38); 107, 299 (312-313).

[22] BVerfGE, NJW 2008, 822 (841).

[23] BVerfGE 35, 202 "Lebach decision".

[24] BVerfGE, NJW 2008, 822 (842).

[25] J. Rux, "Ausforschung privater Rechner durch die Polizei – und Sicherheitsbehorden", (2007) 62 (6) *JuristenZeitung*, 285.

[26] BVerfGE, NJW 2008, 822 (842).

[27] Comunque, questo è ancora oggi tecnicamente impossibile da garantire (Vedi nota 4, a 299).

[28] Vedi BVerfGE 89, 1 (12); 103, 142 (150-151).

[29] BVerfGE 32, 54 (69).

[30] BVerfGE 109, 279 (309, 327).

[31] BVerfGE, NJW 2008, 822 (843).

[32] M. Gercke, "Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit; der Einstaz softwarebasierter Ermittlungsistrumente zum heimlichen Zurgiff auf Computerdaten", (2007) 23 (4) *Computer und Recht*, 245 (250).

[33] BVerfGE, NJW 2008, 822 (841).

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] BVerfGE 65, 1.

[39] BVerfGE 65, 1 (43); 84, 192 (194).

[40] BVerfGE, NJW 2008, 822 (844).

[41] Ibid.

[42] R. Alexy, R. Dreier, 'Statutory Interpretation in the Federal Republic of Germany", in N. MacCormick and R. Summers (eds), *Interpreting Statutes: A Comparative Study* (Darthmouth, Aldershot: 1991) 72-121.

[43] BVerfGE, NJW 2008, 822 (846).

[44] Vedi riguardo una discussione sulla neutralità tecnologica ad esempio, C. Reed, "Taking Sides on Technolgy Neutralità" (2007) 4:3 *SCRIPTed* 263-284.

[45] BVerfGE, NJW 2008, 822 (847).

[46] Ibid.

[47] Ibid.

[48] Per quanto riguarda una discussione sul Cloud Computing vedi: M. Mowbray, "The fog over the Grimpen Mire: Cloud Computing and Law", 6:1 *SCRIPTed* 132-146.

[49] BVerfGE, NJW 2008, 822 (847).

[50] Ibid.

[51] Ibid.

[52] BVerfGE, NJW 2008, 822 (849).

[53] BVerfGE, NJW 2008, 822 (853).

[54] BVerfGE, NJW 2008, 822 (854).

[55] Ibid.

[56] Vedi nota 5.

[57] Consiglio dell'Unione Europea, "Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime", 2987th Justice and Home Affaire Council meeting, 27-28 November 2008, at http://www.ue2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf.

[58] Vedi W. Abel, "Agents, Trojans and tags: The next generation of investigators", (2009) 23:1&2 *International Review of Law, Computers & Technology* 99-108; e W. Abel, B. Schafer " Big Browser Manning the Thin Blue Line – Computational Legal Meets Law Eforcement", (2008) 2 *Problema*, 51-84, per un'analisi più approfondita dei problemi che circondano la ricerca a distanza di computer.

Rubrica: Approfondimenti giuridici